UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/844,924	04/26/2001	Craig S. Skinner	PALM-3609.US.P	8278

49637 7590 04/25/2006

BERRY & ASSOCIATES P.C.
9255 SUNSET BOULEVARD
SUITE 810
LOS ANGELES, CA 90069

EXAMINER	
COLIN, CARL G	
ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 04/25/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/844,924	**Applicant(s)** SKINNER, CRAIG S.
	Examiner Carl Colin	**Art Unit** 2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 February 2006* .

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-31* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *26 April 2001* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)□ The proposed drawing correction filed on _____ is: a)□ approved b)□ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)□ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____ .

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)□ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) □ The translation of the foreign language provisional application has been received.

15)□ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) □ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) □ Interview Summary (PTO-413) Paper No(s). _____ .
5) □ Notice of Informal Patent Application (PTO-152)
6) □ Other: .

DETAILED ACTION

Response to Arguments

1. In response to communications filed on 2/13/2006, the following claims 1-31 are presented for examination.

2. The amendment to the abstract, filed on 2/13/2006 has been considered and the objection to the abstract has been withdrawn.

3. Applicant's remarks, pages 3-7, filed on 2/13/2006, with respect to the rejection of claims 1-31 have been fully considered, but they are not persuasive. Examiner interpreted applicant's argument in the previous response as arguing against the fact that in Beetcher the authorization level is not assigned to the electronic device. Examiner asserted in the previous action with citation that the authorization level is assigned to the electronic device. Regarding claims 1 and 20, Siefert was used to expedite the prosecution to show clearly further evidence that Applicant's claimed limitation "wherein the first authorization level is assigned to the electronic device and authorizes the electronic device to run controlled applications having authorization levels not exceeding the first authorization level" is clearly taught by the prior art. It appears that Applicant has been argued in the response filed on 4/28/2005 and in the present response about "authorizing the controlled device to run <u>controlled applications."</u> Applicant states that Beetcher does not disclose the first authorization level is assigned to the electronic device and authorizes the electronic device to run <u>controlled applications</u> having authorization levels not exceeding the

first authorization level because there exists within Beetcher an assignment between an encrypted entitlement key and a particular distributed software. Examiner respectfully disagrees. The office action states, Beetcher et al. discloses that each customer receives an entitlement key enabling the customer to run only those software modules to which he is entitled (column 4, lines 40-45) that meets the recitation of wherein said first authorization level authorized said electronic device to run controlled applications having authorization levels not exceeding said first authorization level. Beetcher et al. further discloses “Each customer is shipped a generic set of software modules, the entitlement key contains information enabling system to determine which software modules are entitled to execute on it” (column 6, lines 2-7). Beetcher cites,

> “The contents of entitlement key 200 before encryption according to the preferred embodiment are shown in FIG. 2. The key contains charge group field 201, software version field 202, key type field 203, machine serial number field 204, and product entitlement flags 205. Charge group 201 specifies one of 16 possible machine tier values, and is used for supporting tier pricing of software. Software version 202 specifies the version level of the software which is entitled. It is anticipated that separate charges may be imposed for maintenance upgrades of software. The version 202 specified in the key 200 will entitle software at that version level and all previous (lower) levels. Key type field 203 is a reserved area for future changes to the key format, key chaining, or for an extension of the number of different product supported. Machine serial number field 204 contains the serial number of the machine for which the entitlement key is intended. Product entitlement flag 205 is an 80-bit field containing 80 separate product flags, each corresponding to a product number. The bit is set to \`1\` if the corresponding product number is entitled; otherwise it is set to \`0\`.” (column 6, lines 20-40).

Therefore, there is clear evidence that Beetcher discloses the claimed invention as claimed. Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.

Regarding Siefert, Applicant states "Siefert does not disclose or suggest key codes being associated with an electronic device". Examiner respectfully disagrees. Siefert cites,

> "A computer 36 in FIG. 6 is equipped with a key code KC_30. The key code can be burned into Read Only Memory (ROM) which is a part of the hardware of the computer, by the manufacturer of the computer. Alternately, the key code can be buried within the operating system software, in a manner making it difficult to locate. In the latter case, a key code will be assigned to each copy of the operating system software which is delivered, by the manufacturer of the operating system. In either case, the key code is associated with the computer, is readable by the microprocessor (not shown in FIG. 6) contained within the computer, and is stored in a manner designed to impose significant difficulty upon a hacker seeking to learn, or modify, the key code." (Column 6, lines 40-53).
>
> "Presently available software does not contain key codes. In order to allow the computer 36 in FIG. 4 to run such software, several approaches are possible. One is that, upon an order to launch a program, the invention examines the header of the program to be launched, in order to determine the release number, version number, edition number, or equivalent. The invention is equipped with a table for various programs, indicating versions, editions, etc., prior to which no key code is required. If the program to be launched is of a version, edition, etc., requiring no key code, then the program is launched as usual. If the program is of a later version, edition, etc., and does require a key code, then the program is required to pass the security process 45." (column 7, lines 40-55).
>
> The system of Siefert is enabled to "(1) detect when a program launch is requested; then (2) run a security process 45, which compares the key code of the computer with that of the program to be run; then (3) allow launch, if the comparison meets predetermined criteria. Preferably, the security process 45 is located within memory which is not made available to users." (column 8, lines 50-56).

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, there has been teaching, suggestion, and motivation provided in the Office action in the references themselves. To further clarify, Siefert provides a teaching as shown above that uses authorization level assigned to the device to determine whether the device is allowed to run controlled applications (applications that need to pass the security process) while using a security process that is non-accessible to users to prevent hackers from compromising the blockage of programs.

It remains the Examiner's position that claims 1-31 are still rejected in view of Beetcher and Siefert.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4.1 **Claims 1-31** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 5,933,497 to **Beetcher et al.** in view of US Patent 6,526,512 to **Siefert et al.**.

4.2 **As per claims 1 and 20, Beetcher et al.** discloses a method of security comprising the steps of: enabling a computer system to execute a software module with an encrypted entitlement key containing at least a machine serial number and version number that indicates sufficient authority to execute that meets the recitation of a) enabling an electronic device to run a controlled application with an encrypted record containing a copied serial number and a first authorization level, for example (see column 6, lines 20-67); **Beetcher et al.** discloses that each customer receives an entitlement key enabling the customer to run only those software modules to which he is entitled (column 4, lines 40-45) that meets the recitation of wherein said first authorization level authorized said electronic device to run controlled applications having authorization levels not exceeding said first authorization level. **Beetcher** also discloses other entitlements such as charge group, key type, serial number of the machine, and product entitlement field assigned to the device (see column 6, lines 20-40). In another embodiment, Beetcher discloses in column 7, lines 1-16, other authorization levels that are hardware specific assigned to said electronic device. There is suggestion in column 2, lines 49-53 that other entitlement may also be machine specific entitlement or authorization level assigned to a machine to make sure that a software is authorized to run on a specific machine. b) verifying said electronic device is correctly enabled, for example (see column 6, line 65 through column 7, line 47); and c) verifying said first authorization level is of sufficient authority to run said controlled application on said electronic device, for example (see column 6, line 65 through column 7, line 47); and wherein a second authorization level of said controlled application does not exceed the first authorization level (column 7, lines 1-65). **Beetcher et al** suggests to add protection by using entitlement that contains machine specific information and encoding it into the software itself. **Siefert et al.** in an analogous art teaches key codes containing authorization levels (column 2, lines 40-65) and the key codes (authorization levels) are assigned to an electronic device and authorizes said electronic device to run controlled applications having authorization levels not exceeding said first authorization level (see column 4, line 44 through column 5, line 55). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Beetcher et al** to include the step of wherein the first authorization level is assigned to the electronic device and authorizes the electronic device to run controlled applications having authorization levels not exceeding the first authorization level as taught by **Siefert et al** (see column 4, line 44 through column 5, line 55). One of ordinary skill in the art would have been motivated to do so because the teaching of Siefert provides detecting and controlling any program that is required to pass the security process by doing the following: when a program launch is requested, running a key code process of comparing the key code of the computer with that of the program to be run in order to authorize execution of the program upon meeting predetermined criteria. One of ordinary skill in the art would have recognized the advantage of preventing hacker from learning the identities of the key codes and preventing hacker from learning how the security process run by assigning key codes (authorization levels) to both the computer and the program by a match determination process and using region of memory non-accessible to users to store the key codes (authorization levels) as suggested by **Siefert et al** (column 7, lines 15-25 and column 7, line 50 through column 8, line 35 and column 8, lines 50-67).

As per claims 2, 14, and 21, Beetcher et al. discloses the limitation of wherein step a) comprises the steps of: al) fetching a serial number uniquely associated with said electronic device, said serial number located on said electronic device, for example (see column 7, line 47); a2) copying said serial number, forming said copied serial number that is identical to said serial number, for example (see column 6, lines 20-40); a3) creating a record that contains said copied serial number and said first authorization level, said first authorization level previously assigned to said electronic device, for example (see column 6, lines 20-40); a4) encrypting said record, forming said encrypted record, for example (see column 4, lines 57-65 and column 8, lines 53-65); and a5) storing said encrypted record in said electronic device, for example (see column 8, lines 53-65). These claims are also rejected on the same rationale as the rejection of claim 1 for reciting "said first authorization level previously assigned to said electronic device".

As per claims 3 and 22, Beetcher et al. discloses the limitation of wherein step b) comprises the steps of: bl) locating said encrypted record, for example (see column 9, line 40 through column 10, line 20); b2) decrypting said encrypted record, if said encrypted record is located, for example (see column 9, line 40 through column 10, line 20); b3) reading said copied serial number from said encrypted record, if said encrypted record is successfully decrypted; b4) fetching said serial number, for example (see column 9, line 40 through column 10, line 20); and b5) comparing said serial number and said copied serial number, for example (see column 9, line 40 through column 10, line 20 and column 13, lines 1-8).

As per claims 4 and 23, **Beetcher et al.** discloses the limitation of wherein step b) comprises the further step of executing said controlled application on said electronic device, said controlled application having controlled attributes, for example (see column 6, lines 40-67);

As per claims 5, 12, 24, and 31, the combination of **Beetcher et al** and **Siefert et al** discloses the limitation of wherein said step c) comprises the steps of: c1) reading said first authorization level from said encrypted record that is decrypted, if said serial number and said copied serial number match, for example (see **Beetcher et al,** column 9, lines 40-67 and column 10, lines 20-67); c2) comparing said first authorization level with a second authorization level assigned to said controlled application **(Beetcher et al**, column 10, lines 40-4 and column 7); and c3) allowing access to said controlled attributes of said controlled application, if said first authorization level is of an equal or higher authorization level than said second authorization level, for example (see **Beetcher et al**, column 10, lines 20-47 and column 4, lines 34-46). **Siefert et al** also discloses comparing first authorization level with second authorization level to authorize the computer to run controlled applications as discussed in claim 1. Therefore, these claims are also rejected on the same rationale as the rejection of claim 1.

As per claims 6, 15, and 25, **Beetcher et al.** discloses the limitation of wherein step a) is performed with object code instructions that meet the recitation of an enabler application, said enabler application enabling said electronic device to run applications having authorization levels equal to or lower than said first authorization level, for example (see column 8, lines 48-67 and column 4, lines 34-46).

As per claims 8, 9, 18, 19, 27, and 28, the combination of **Beetcher et al** and **Siefert et al** discloses the limitation of comprising the further step of: aborting said application and denying access if any of the following conditions are met: said encrypted record is not successfully located in step b1) ; said encrypted record is not successfully decrypted in step b2); said serial number and said copied serial number do not match in step b5); or said first authorization level is of a lesser value than said second authorization level in step c2) , for example (see **Beetcher et al**, column 8, lines 48-67 and column 4, lines 34-46 and column 10, lines 20-67).

Claims 13 and 16 contain some of the limitations of the rejected **claims 1-5**. Therefore, **claims 13 and 16** are rejected on the same rationale as the rejection of **claims 1-5**.

As per claim 17, **Beetcher et al.** discloses the limitation of wherein the same encryption/decryption protocol is used in performing steps c) and m), for example (see column 13, lines 5-18).

As per claims 7 and 26, Beetcher et al. substantially teaches the claimed method of claims 6 and 25. **Beetcher et al.** does not explicitly teach removing said enabler application from said electronic device after successfully completing step a). However, **Siefert et al.** in an analogous art teaches control access to enhance security of resources where a match determination process can take actions of erasing part or all of the program to defeat running of the program, for example (see column 7, lines 35-40). **Siefert et al.** also adds, hiding process/codes or removing or placing them in separate memory or non-accessible memory locations can prevent hackers to trace the logic of codes, for example (see column 7, line 40 through column 8, line 5). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Beetcher et al.** to remove said enabler application from said electronic device after successfully completing step a) as taught by **Siefert et al**. One skilled in the art would have been lead to make such a modification because it would make the security process non accessible to hackers, as suggested by **Siefert et al** for example (see column 7, line 40 through column 8, line 35).

As per claims 10-11 and 29-30, Beetcher et al. discloses locking in memory the version number the product number, serial number etc. and also discloses codes stored in read-only memory (ROM) to make it not capable of alteration by customers, for example (see column 7, lines 15-30 and column 9, lines 49-67). It is well known in the art of computer security that computers have flash memory and using a flash memory will not depart from the spirit and scope of the invention of **Beetcher et al.**. **Siefert et al.** also discloses using read-only memory (ROM) for the encrypted data and serial number. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to store said encrypted record and serial number in locked flash record in said electronic device as suggested by **Beetcher et al.** One skilled in the art would have been lead to make such a modification to prevent alteration of these data by customers.

Conclusion

5. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

5.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Carl Colin
Patent Examiner
April 17, 2006

CHRISTOPHER REVAI
PRIMARY EXAMINER
4/24/06